Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at http://about.jstor.org/participate-jstor/individuals/early-journal-content.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact support@jstor.org.

GROUPS OF THE FUNDAMENTAL OPERATIONS OF ARITHMETIC

By G. A. Miller

By adding n to x_1, then this sum to x_1, etc., there results an infinite series of numbers*, $n, n + x_1, n + 2x_1, \cdots$. If these numbers are taken with respect to a given modulus (m) only m/d of them are distinct, d being the highest common factor of m and x_1. These distinct numbers are of the form $n + kd, k = 1, 2, \cdots, m/d$. If n_0 represents the smallest one with respect to modulus m, their least positive residues are $n_0 + kd$, $k = 1, 2, \cdots, m/d$. These elementary principles of number theory will be frequently employed in the following developments.

Instead of adding n to one number we may add it to a series of numbers $x_1, x_2, \cdots, x_l$. If the sums thus obtained are again added to this series in any order, and these operations are repeated, the resulting numbers again belong to m/d distinct classes with respect to modulus m, d being the highest common factor of $x_1, x_2, \cdots, x_l, m$. Their least positive residues are again given by $n_0 + kd$, $k = 1, 2, \cdots, m/d$, where n_0 is the smallest number with respect to modulus m that is obtained by the given operations.

As the definitions of a group clearly apply to these operations and as all the numbers are obtained by a repetition of the same operation, it is convenient to say that *adding to one or more given numbers and taking the results with respect to a fixed modulus gives rise to the cyclic group whose order is equal to the number of least positive residues of all the resulting numbers.* For instance, when $n = 8, x_1 = 15, m = 20$, the least positive residues of the resulting numbers are 3, 8, 13, 18. These become the cyclic group of order 4 when they are increased successively by some multiple of $d = 5$. These results remain unchanged by adding $x_2 = 35$ to the given conditions, but if $x_2 = 12$ the cyclic group becomes of order 20 since $d = 1$ in this case.

---

* All the numbers employed will be regarded as positive integers unless the contrary is stated.

These considerations are so elementary that they offer little interest in themselves. They are explicitly stated, partly for the sake of completeness and partly on account of their fundamental importance in the following developments. It should be carefully observed that we add only to $x_1, x_2, \cdots, x_l$. If the resulting numbers were added together, the order of the cyclic group would be m/d', d' being the highest common factor of d and n. The fundamental thought in what precedes is that *the groups of addition are cyclic*. We proceed to consider subtraction. It will appear that its groups are of the dihedral rotation type.

1. Groups of subtraction. If we subtract n from x_1 the resulting number $(x_1 - n)$ may be supposed to take the place of either x_1 or n. In the former case subtraction is an operation of infinite period unless we consider a modulus; in the latter case it is of period two, since $x_1 - (x_1 - n) = n$. We shall here adopt the latter point of view and hence regard subtraction from x_1 as a reflection on the point $x_1/2$, the numbers being represented in the usual manner by points on a line.

Subtracting n from x_1 and then subtracting the resulting number from x_2 is equivalent to reflecting n on the point $x_1/2$ and then reflecting $x_1 - n$ on the point $x_2/2$. The result is equal to a translation through $x_2 - x_1$; that is, n becomes $n + (x_2 - x_1)$. It was seen above that these translations with respect to modulus m generate the cyclic group of order m/d, d being the highest common factor of $x_2 - x_1$ and m. Hence the operations of subtracting from x_1 and x_2 generate the dihedral rotation group of order $2m/d$.* One of the most interesting examples along this line is furnished by taking the complement and the supplement of an angle. As these two operations are equivalent to a rotation through $\pi/2$ they generate the group of order 8 which is identical with the group of movements of the square.† It contains two operators of period 4, five of period 2, and the identity.

While the general theory of the group obtained by subtracting from two numbers follows directly from the theory of the groups which are generated by two operators of order two, yet it seems desirable to add a few details with respect to the special problem on hand. A reflection followed by a translation is equivalent to a reflection of the original point on the point obtained by moving the original point of reflection through half the translation. Hence a reflection followed by a translation is always of period two, and a reflection followed by a translation followed by the same reflection is the inverse of the translation. In other words a translation is transformed into its inverse by any reflection. Hence the order of the group generated by *any* translation and a reflection is twice the order of the group generated by the translation alone. When the translation is equal to two given reflections the group generated by the translation and one of these reflections includes the other reflection.

---

* *Bulletin of the American Mathematical Society*, vol. 7 (1901), p. 424.

† Davis, *Nebraska University Studies*, vol. 4 (1904), p. 231.

When n is subtracted from a series of numbers $x_1, x_2, \cdots, x_l$ and the remainders are again subtracted from these numbers, in any order, these operations of order 2 generate the dihedral rotation group of order $2m/d$, where d is the highest common factor of m, and of all the differences of the form $x_\alpha - x_\beta$. This follows immediately from the fact that the translations which are equivalent to the pairs of these reflections generate the cyclic group of order m/d. As there are just two positive points less than m with respect to which all reflections are equivalent modulo m, there are just $2m/d$ different values of n modulo m which go into less than $2m/d$ distinct numbers by the operations of the group of subtraction. Each of these special values goes into m/d distinct values, differing by multiples of d, under this group; *i. e.* these $2m/d$ special values constitute two sets such that all of those of one set go into each other under the group.* Congruent numbers modulo m go into congruent numbers under all of these operations.

2. Groups of multiplication and groups of division. Since the groups of multiplication have received considerable attention † it seems necessary to do little more here than state those results which are fundamental in the study of the groups of division. There is, however, one important principle connected with these groups which has not received sufficient attention; viz. the *necessary* condition that a set of numbers becomes a group when they are combined according to multiplication. It has been observed that a sufficient condition is the fact that the set is composed of all the numbers which are less than a given modulus (m) and prime to m. That this condition is not necessary follows directly from the fact that the four numbers 2, 4, 6, 8 become a group when their products are taken with respect to modulus 10.

---

* For example, by taking the complement and the supplement we obtain 8 distinct angles from a given angle provided it is not a multiple of $\pi/4$. In the latter case only 4 distinct angles, differing by $\pi/2$, are obtained by these operations.

† *Cf.* ANNALS OF MATHEMATICS, ser. 2, vol. 2 (1901), p. 77.

The necessary and sufficient condition that a given set of numbers, which are distinct with respect to modulus m, generates a group with respect to multiplication is that the highest common factor of the modulus and a number of the set is independent of the choice of this number, and that m divided by this highest common factor is prime to this factor. That this condition is sufficient follows directly from the fact that by dividing by the highest common factor we obtain a set of numbers each of which is prime to the new modulus. The condition is also necessary to insure that every number of the set can be obtained by combining any other number of the set with numbers of the set. For example, 5, 35 generate the four-group 5, 25, 35, 55 mod 60; while 5, 25 generate the group of order 2 with respect to the same modulus. In both of these groups 25 corresponds to the identity. In general, the number which is congruent to unity, modulo m divided by the common factor, corresponds to the identity.

When the elements of a group are not prime to the modulus the group is identical with the one obtained when these elements and the modulus are divided by their highest common factor. In other words, all multiplication groups can be represented by elements which are prime to the modulus. Hence this special class of abelian groups is identical with the groups and the sub-groups of the groups of isomorphisms of cyclic groups, whose properties may be assumed to be known.* We proceed to the groups of division and shall find that these are obtained by simply adding operators of period two to the groups of multiplication.

The period of the operation of division as that of subtraction depends upon the point of view. In each case the group may be regarded as the same as

---

*ANNALS OF MATHEMATICS, *loc. cit.*; Lucas, *Théorie des nombres*, 1891, p. 395.

that of the corresponding direct operation. That is, we may regard subtraction as an operation on the minuend so that the remainders become new minuends. From this standpoint there is no difference between the group of subtraction and that of addition. Similarly, if we regard the quotients as new dividends there is no essential difference between the group of division and that of multiplication. If, however, the quotient is regarded as a new divisor, the operation of division is always of period two, instead of being of a finite period only when a modulus is employed. In what follows division will be regarded as of period two.

Geometrically the operation of dividing x_1 by n may be regarded as an inversion of n followed by a stretching in the ratio x_1. That is, any point n goes into the point x_1/n by this operation.* It is geometrically evident that this operation is of period two. By dividing two distinct numbers x_1, x_2 there result two operations of period two whose group will now be considered. The product of these two operations, in order, brings n into $(x_2/x_1)n$. If each of the numbers x_1, x_2 is prime to m there will be just one number (x_3) less than m such that $x_2 \equiv x_1 x_3 \bmod m$.† We shall regard x_2/x_1 and x_3 as equal with respect to modulus m. Hence the powers of x_2/x_1 constitute a cyclic group modulo m and the two operations x_1/n, x_2/n generate a dihedral rotation group whose order is twice the order of this cyclic group.

The general case of dividing the l distinct numbers $x_1, x_2, \cdots, x_l$ by n presents scarcely any new considerations. If m is prime to all the numbers $x_1, x_2, \cdots, x_l$ the group (G) generated by these l operations of period two is obtained by adding operations of order two to the group (H) of multiplication generated by the quotients $x_1/x_2, x_1/x_3, \cdots, x_2/x_3, \cdots, x_{l-1}/x_l$. The order of G is twice the order of H, and the additional operations of order two transform each operator of H into its inverse. That is, this group consists of an abelian group, which is found in the group of order $\phi(m)$ generated by all the numbers less than m and prime to m, and as many more operators of period two as there are in this abelian group.

If one of the numbers $x_1, x_2, \cdots, x_l$ occurs among the quotients x_1/x_2,

---

* This clearly remains true even when the numbers are complex.

† This is also true when m, x_1 and m, x_2 have the same highest common factor (d) and m/d is prime to d, as is evident from the preceding developments. For brevity we shall not mention this evident extension in what follows.

$x_1/x_3, \cdots, x_2/x_3, \cdots, x_{l-1}/x_l$ then all of them are found among these quotients. Hence the coefficients of n and $1/n$ involve either g or $g/2$ distinct numbers modulo m, g being the order of G, and n goes into g or $g/2$ distinct values under G as x_1 does not or does belong to H. For instance, by dividing 2 and 6 by n modulo 11 the following ten distinct coefficients result:* n, $4n$, $5n$, $9n$, $3n$, $\frac{2}{n}$, $\frac{2}{4n}$, $\frac{2}{5n}$, $\frac{2}{9n}$, $\frac{2}{3n}$. No new numbers are obtained by dividing 6 by these numbers since $\frac{6}{n} = \frac{2}{4n}$, $\frac{6}{4n} = \frac{7}{n} = \frac{2}{5n}$, etc. For special values of n these numbers become a group modulo m only when n is equal to one of the given coefficients. The order of this group is equal to the number of distinct coefficients. The prominent thought of this section is that the group of division is obtained from the corresponding group of multiplication in the same way as the group of subtraction is derived from the corresponding group of addition.

3. Groups of subtraction and division. Since the operations of dividing x_1 by n and of subtracting n from x_1 (x_1/n, $x_1 - n$) are of period two, it is of interest to inquire into the group generated by them. As is well known the six values of the anharmonic ratio are obtained from any one of them by a repetition of these two operations when $x_1 = 1$.† Similarly, each of the six trigonometric functions ($\sin^2 x$, $\cos^2 x$, $-\tan^2 x$, $-\cot^2 x$, $\sec^2 x$, $\csc^2 x$) is obtained from any one of them by the same operations. That is, the operations of inversion and subtraction from unity generate the symmetric group of order six. Since these two operations performed in succession are equivalent to an operation of period three, this result follows directly from the theory of the dihedral rotation groups.

When $x_1 = 2$, the given operations lead to another well known group; viz., the group of movements of the square. This follows directly from the fact that the two successive operations $2/n$ and $2 - n$ are equivalent to the operation $\frac{2}{2-n}$ which is of period 4. In fact, $\left(\frac{2}{2-n}\right)^2 = 2 \Big/ \left(2 - \frac{2}{2-n}\right) = \frac{2-n}{1-n}$, and $\left(\frac{2-n}{1-n}\right)^2 = n$. When $x_1 = 3$, there results the dihedral group of order 12 since $\frac{3}{3-n}$ is of period six.[*] It is easy to prove that this group is of infinite order for every larger value of x_1.

---

* For convenience the unknown (n) is also given.

† *Cf.* Burnside, *Theory of groups of finite order*, 1897, p. 18.

The last statement may be proved as follows: Let $s_1 = x_1 - n$, $s_2 = \frac{x_1}{n}$. Then will $s_1 s_2 = x_1 - \frac{x_1}{n}$, $(s_1 s_2)^2 = \frac{x_1 - (x_1 - 1)n}{1 - n}$. In general let $(s_1 s_2)^k = \frac{\alpha + \beta n}{\gamma + \delta n}$. Then will $(s_1 s_2)^{k+1} = \frac{\beta x_1 - (\alpha + x_1 \beta) n}{\delta x_1 - (\gamma + \delta x_1) n} = \frac{\alpha' + \beta' n}{\gamma' + \delta' n}$. If the value of each of the fractions β/α, δ/γ lies between $-\frac{1}{2}$ and -2 and if $x_1 \geqq 4$ then will the fractions $\frac{\beta'}{\alpha'}$, $\frac{\delta'}{\gamma'}$, satisfy the same conditions. As these conditions are satisfied in $(s_1 s_2)^2$, they must be satisfied for the higher powers. That is, the two operations in question generate a group of infinite order whenever $x_1 \geqq 4$. For negative values of x_1 the ratios β'/δ', δ'/γ' are negative and not zero whenever β/δ, δ/γ satisfy these conditions. Hence $s_1 s_2$ is also of an infinite period for all negative values of x_1.

From the same substitutions it follows also directly that $s_1 s_2$ is of an infinite period whenever x_1 is a proper fraction; for, if α, β involve the same highest power of x_1 and if the coefficient of this power is unity in each of these terms then will the same be true of α', β'. It is evident that these remarks apply equally to γ, δ and γ', δ'. It should be observed that the groups of this section are independent of any modulus while all of those which precede, with exception of the trivial group of order two, are dependent upon a modulus.

---

[*] These examples are special cases of the following general theorems: whenever $x_1^2 = x_2$ the operations of substracting n from x_1 and dividing x_2 by n give rise to the symmetric group of order 6; when $x_1^2 = 2x_2$ these operations lead to the octic group, and when $x_1^2 = 3x_2$ they generate the dihedral rotation group of order 12. When $x_1 = 0$ while x_2 has any other given value, there results the group of division and change of sign. This is evidently the well known four-group. When x_1, x_2 do not satisfy any of these conditions, the two given operations cannot generate a finite group which transforms every rational point of the plane into a rational point. Hence these four-groups are of fundamental importance in the theory of point transformations of the plane. The examples given above illustrate these groups when $x_1 = x_2$.

While it is well known that the same group frequently presents itself in many different investigations, yet it may be in place to emphasize the fact that the octic group is the group of taking the supplement and the complement of an angle, of dividing 2 by *n* and subtracting *n* from 2, of the movements of solid space which transform a square into itself, of the three valued function in four letters, of the substitutions in four letters which transform the cyclic group in these letters into itself, of isomorphisms of itself, of subtracting *n* from 3 and 6 modulo 12, of dividing 1 and 2 by *n* modulo 5, etc. The number of such illustrations is always infinite but in this case some seem to be of especial interest.